

Remarks

Claims 1, 6, 7, 9, 12, 14, 16, 17, 19, 20, 23-25, 30-33, 42, 43, 47-50, 72-74, 79, 80, 80, 82 and 84-86 have been amended. Claims 2, 15, 46 and 78 have been canceled. Claims 87-92 have been added. Claims 1, 3-14, 16-45, 47-52, 72-77 and 79-92 are pending in the application. Reconsideration of the rejections and objections at an early date is requested.

Support for the claim amendments and new claims may be found, at least, as follows:

Claim 1: p. 8 [0030] – p. 9 [0032]; p. 12 [0048]; p. 13 [0056] – [0057]; p. 14 [0059]; p. 17 [0072]; p. 18 [0074]; p. 26, claim 48

Claim 12: p. 8 [0030]

Claim 14: p. 13 [0054]; p. 19 [0077]

Claim 16: p. 13 [0055]; p. 17 [0070] – [0071]; p. 19 [0076] – [0077]

Claims 48, 49, 50, 85 and 86: similar to claim 1

Claim 87: p. 13 [0055]

Claim 88: p. 11 [0046]; p. 13 [0054]

Claim 89: p. 18 [0074]

Claim 90: p. 18 [0074]

Claim 91: p. 9 [0035]; p. 11 [0045] – [0046]

Claim 92: p. 10 [0038]; p. 13 [0056]

Claims 1-4, 6-12, 14-26, 28, 30, 32, 34-37, 41-52, 72-82 and 84-86 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Michener* (U.S. Publication No. 2002/0198848) in view of *Robinson* (U.S. Publication No. 2003/0061172).

The examiner suggests that *Michener* discloses all of the features of claims 1, 48 & 49, except registering a user, which the examiner suggests is disclosed in the abstract of *Robinson*. The examiner contends that it would have been obvious to combine the teachings of these documents thereby rendering the invention obvious. Applicant respectfully submits that *Michener* does not contain a disclosure of the all of the features said to be present by the examiner.

In *Michener* the token (calculator) 100 generates a passcode/transaction code/token ID 18', and the verification server 22 verifies the passcode/transaction code/tokenID 18' (Fig. 1). In contrast, the claims require both of these steps to be performed by the transaction manager. It is neither disclosed nor obvious for the steps of:

- generating a single use transaction request identification with a transaction manager;
- storing the generated single use transaction request identification in a relationship with an identifier of a registered user and banking information of the registered user in a storage of the transaction manager; and

- checking the validity of the received transaction request identification with the transaction manager apparatus and disabling re-use of the request identification;

because *Michener* does not disclose that both the generating and checking steps are performed with the transaction manager. Further, *Michener* does not disclose both generating and storing step are performed with the transaction manager – indeed *Michener* does not disclose a storing step at all in the passage cited by the examiner. Further, it would not be obvious to combine a portable device carried by the user (the token) with an apparatus operated by a credit card issuer (the verification server) into a single apparatus (the transaction manager).

In paragraph 34 of *Michener* it states that the composite passcode 18' is provided by the merchant to the bank; whereas claim 1 requires “receiving at the transaction manager apparatus a payment request” and then “sending an EFT request to a financial institution system,” which clearly indicates that the transaction manager is not a bank, but an intermediary system. Thus, disclosure of providing a passcode to a bank is not the same receiving at the transaction manager apparatus a payment request.

Furthermore, in claim 1 the EFT request is required to be sent after the received transaction request identification is valid, whereas in *Michener* the verification happens as part of the EFT request (after the request is received by the bank). In particular, in claim 1 the EFT request is send to

the financial institution (bank) after verification of the transaction request by the transaction manager, whereas in *Michener* the bank sends the passcode to the verification server. Thus, the checking step (determining step, as amended) is not disclosed or suggested in *Michener*.

Paragraph 36 of *Michener* describes that the verification server sends a verification status to the bank. This is not equivalent to sending an EFT request to a financial institution because an EFT request necessarily comprises the source and recipient accounts (banking information) and the value of the transaction, whereas a verification status message does not include this information and the bank in *Michener* already has this information. Thus, the sending of an EFT request step of claim 1 is not disclosed or suggested in *Michener*.

Also, because the verification server sends the bank a verification status, there is no disclosure of receiving at the transaction manager apparatus confirmation of the transfer from the financial institution when the transfer is performed because the status is sent in the other direction in *Michener*.

For the above reasons *Michener* does not have the features said to be present by the examiner. Consequently, the combination of *Michener* and *Robinson* does not render claim 1 obvious.

By virtue of the novelty and non-obviousness of claim 1, the claims dependent thereon are also novel and not obvious. However, Applicant does not agree with other aspect of the examiner's report and without prejudice to other rebuttals that may be available, certain selected claims are discussed further below.

With regard to claim 3, this requires that the transaction request identifier is a random number. In paragraph 40 *Michener* discloses a random challenge communicated back to the user. Clearly, the use of the word back indicates that the transaction request has already been sent and this is an additional step. The random challenge is therefore not a substitution of the transaction request identifier in the claims. Furthermore, there is no disclosure of storing the generated single use transaction request identification in a relationship with an identifier of a registered user and banking information of the registered user in a storage of the transaction manager.

With regard to claim 14, this requires the payment request to further comprises a component provided by the registered user and that the transaction manager apparatus receive the user provided component from the user independently from and before receiving the purchase request, and storing of

the user provided component in the storage in a relationship with the identifier of the registered user. This is not disclosed in *Michener* despite the assertion that it is disclosed in paragraph 24. *Michener* discloses sending the passcode (which is a digest of credit card number, transaction amount and transaction count), transaction count and token ID in composite passcode 18' to the bank (Fig. 1). However, not only is the bank not a transaction manager apparatus, none of the components of the transaction request are a component provided to the transaction manager by the registered user independently from and before receiving the purchase request.

With regard to claim 16, this requires comparing the user provided component received in the payment request with the stored user provided component to determine the validity of the payment request. While in *Michener* there is a comparison of the transaction count 117 to the previous transaction count 117", the transaction count is not a user provided component, and therefore there is no comparison of a user provided component. Consequently there is no disclosure of claim 16.

Claim 17 requires that the user provided component comprise a secret identification of the user known to the registered user. Paragraph 41 of *Michener* discloses a PIN 112 used to unlock the token. There is no disclosure of the PIN being a user provided component sent in the payment request. Thus, there is no disclosure of claim 17 in *Michener*.

Claim 18 requires a transaction limit and with a transaction limit override password. While Robinson may describe a transaction limit, there is no disclosure of a transaction limit override password.

Claim 26 requires combining the transaction request identification and the user provided component by hatching. *Michener* makes no disclosure of hatching.

Claim 28 requires that the user provided component comprises a secret identification of the user known to the registered user and recorded in the financial institution. Paragraph 41 of *Michener* discloses a PIN 112 used to unlock the token. There is no disclosure of the PIN being a user provided component sent in the payment request or that the PIN is known to the financial institution (bank). Thus, there is no disclosure of claim 28 in *Michener*.

Claim 32 requires that the confirmation message sent from the transaction manager apparatus to the recipient be the same as the confirmation of the transfer received from the financial institution. Not only does *Michener* not sent a confirmation message from the financial institution (bank) to the

transaction manager, but the status sent is different, not the same (SUCCESSFUL changes to APPROVED and UNSUCCESSFUL changes to DISAPPROVED).

Claim 37 requires sending a confirmation of the transfer of funds from the transaction manager apparatus to the registered user. Paragraph 48 of *Michener* describes sending a confirmation message to the merchant, but there is no description of sending a confirmation of the transfer of funds from the transaction manager apparatus to the registered user.

Claim 41 requires that sending the transaction request identification to the registered user comprises sending the transaction request identification to a portable storage device held by the user. Paragraph 34 of *Michener* describes a composite passcode 18' being provided by the user to the merchant and the merchant then providing it to the bank. In paragraphs 28 and 29 of *Michener* the composite passcode 18' is described as being generated by the token 100. Nowhere in *Michener* is there a description of sending the passcode 18 to the token (portable storage device).

Claim 47, as amended, requires sending the EFT request from the transaction manager apparatus to the financial institution comprising selecting the financial institution from a plurality of financial institutions according to the banking information retrieved according to the payment request after the payment is validated. The examiner notes that *Robinson* discloses the consumer selecting the type of financial account. However, this is not selecting the financial institution from a plurality of financial institutions according to the banking information retrieved according to the payment request after the payment is validated. Therefore, the feature of claim 47 is not disclosed by *Robinson*.

Claims 75 and 76 require identifying the registered user when a remotely located electronic device of the registered user connects to the transaction manager apparatus and generation of the single use transaction request identification occurs when the registered user is identified. *Michener* describes a token 100 which is in possession of the user. However, the token does not connect to the verification server, nor is the user identified when the connection occurs. Instead, *Michener* requires the user enter a PIN into the token to identify the user.

With regard to claim 13 the examiner takes official notice that it is old and well known in the banking arts to confirm a valid bank account before complete registration. Applicant disputes the veracity of this assertion because the examiner has provided no citation for this assertion and the

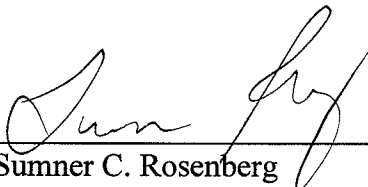
relevance to this claim. This claim requires registration of a user with a third party authenticator and for the third party authenticator to confirm the bank account is valid. The examiner's official notice makes no mention of this.

With regard to claims 27 and 29 the examiner takes official notice that it is old and well known in the banking art to have a one-time transaction number in a used transaction number list to ensure they are not reused. The examiner has provided no support for this assertion and the applicant contends that this is not in fact the case, in the absence of any evidence to the contrary. A similar contention is made with regard to the official notice mentioned in relation to claim 83.

In view of the comments above, Applicant respectfully requests an allowance of the pending claims at an early date.


A Credit Card Payment submitted via EFS-Web authorizing payment in the amount of \$470.00, representing \$65.00 for a small entity under 37 C.F.R. § 1.17(a)(1) for a one month extension of time and \$405.00 for a small entity under 37 C.F.R. § 1.17(e), a Request for Extension of Time, Supplemental Information Disclosure Statement, Statement List and a Request for Continued Examination are enclosed. This fee is believed to be correct, however, the Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 14-0629.

Respectfully submitted,



Sumner C. Rosenberg
Registration No. 28,753

BALLARD SPAHR LLP
Customer Number 23859
(678) 420-9300 Phone
(678) 420-9301 Fax

CERTIFICATE OF ELECTRONIC TRANSMISSION UNDER 37 C.F.R. § 1.8			
I hereby certify that this correspondence, including any items indicated as attached or included, is being transmitted via electronic transmission via EFS-Web on the date indicated below.			
Name of Person (Print/Type)	Montrell Doster		
Signature		Date	April 2, 2010